CLAIMS

What is claimed is:

1 A method for controlling access to file on a server over a network, the method comprising the steps of:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file;

(d) generating a ticket that includes an identifier identifying the particular file on the second server if the user has been granted authorization access;

(e) creating a redirect URL ticket to the file on the second server by

(i) modifying the client's URL request to identify the second server, and

(ii) augmenting the URL request with the ticket authorizing access to the particular file; and

(f) returning the redirect URL ticket to the client, such that the client uses the redirect URL to request the file from the second server.

2 The method of claim 1 further including the step of:

(g) verifying the ticket on the second server and returning the requested file.

3 The method of claim 1 wherein step (c) further includes the step of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

4 The method of claim 1 wherein step (a) further includes the step of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

5 The method of claim 4 wherein step (a) further includes the step of: allowing the access controls to be specified before and after the file is replicated onto the second server.

6 The method of claim 4 wherein step (a) further includes the steps of: storing the name of the file in a database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

7 The method of claim 1 wherein step (e) further includes the step of: generating the URL ticket in the form:

scheme://servername/.../basedir;*parameters*/subdir/.../file.extension.

8 The method of claim 7 wherein step (e) further includes the step of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

9 The method of claim 7 wherein step (e) further includes the step of: binding a combination of "basedir+path+sessionid" to an IP address of the client at first use of the URL ticket.

10 The method of claim 9 wherein step (g) further includes the step of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

11 The method of claim 1 further including the step of: ensuring that only the client that was issued the URL ticket can use the URL ticket by

(i) issuing a transfer ticket from the first server to the client when the first server needs to redirect the client to the second server,

(ii) recognizing by the second server the transfer ticket in a request from the client,

(iii) redirecting the client back to the second server with a URL ticket, and

(iv) verifying the ticket on the second server and returning the requested file.

12 The method of claim 1 further including the step of providing a content server as the first server and providing at least one replica server as the second server.

13 A system for controlling access to file on a server over a network, the system comprising the steps of:

means for allowing a content originator to publish a file on a first server and to specify what users are authorized to access to the file, wherein files on the first server are replicated on a second server;

means responsive to receiving a URL request from a client for a file from the first server for determining if a user of the client has been granted authorization to access the file;

means for generating a ticket that includes an identifier identifying the particular file on the second server if the user has been granted authorization access;

means for creating a redirect URL ticket to the file on the second server by modifying the client's URL request to identify the second server, and augmenting the URL request with the ticket authorizing access to the particular file; and

means for returning the redirect URL ticket to the client, such that the client uses the redirect URL to request the file from the second server.

14 The system of claim 13 further including means for verifying the ticket on the second server and returning the requested file.

15 The system of claim 13 wherein the client comprises a web browser that has not been customized to request tickets.

16 The system of claim 13 wherein the content originator specifies what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

17 The system of claim 16 wherein the access controls can be specified before and after the file is replicated onto the second server.

18 The system of claim 16 wherein a name of the file is stored in a database along with the access privileges specified for the file, and when a user makes a request to access the file, the name of the file is looked up in the database to determine if the user

has been granted access to the file.

19 The system of claim 13 wherein the URL ticket is in the form:

scheme://servername/.../basedir;*parameters*/subdir/.../file.extension.

20 The system of claim 19 wherein the URL ticket includes a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

21 The system of claim 20 wherein a combination of "basedir+path+sessionid" is bound to an IP address of the client at first use of the URL ticket.

22 The system of claim 21 wherein the URL ticket is verified as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

23 The system of claim 13 wherein it is ensured that only the client that was issued the URL ticket can use the URL ticket by

(i) issuing a transfer ticket from the first server to the client when the first server needs to redirect the client to the second server,

(ii) recognizing by the second server the transfer ticket in a request from the client,

(iii) redirecting the client back to the second server with a URL ticket, and

(iv) verifying the ticket on the second server and returning the requested file.

24 The system of claim 13 wherein the first server comprises a content server and the second server comprises at least one replica server.

25 A computer-readable medium containing program instructions for controlling access to file on a server over a network, the program instructions for:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file;

(d) generating a ticket that includes an identifier identifying the particular file on the second server if the user has been granted authorization access;

(e) creating a redirect URL ticket to the file on the second server by

(i) modifying the client's URL request to identify the second server, and

(ii) augmenting the URL request with the ticket authorizing access to the particular file; and

(f) returning the redirect URL ticket to the client, such that the client uses the redirect URL to request the file from the second server.

26 The computer-readable medium of claim 1 further including the instruction of:

(g) verifying the ticket on the second server and returning the requested file.

27 The computer-readable medium of claim 1 wherein instruction (c) further includes the instruction of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

28 The computer-readable medium of claim 1 wherein instruction (a) further includes the instruction of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

29 The computer-readable medium of claim 4 wherein instruction (a) further includes the instruction of: allowing the access controls to be specified before and after the file is replicated onto the second server.

30 The computer-readable medium of claim 4 wherein instruction (a) further includes the instructions of: storing the name of the file in a database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

31 The computer-readable medium of claim 1 wherein instruction (e) further includes the instruction of: generating the URL ticket in the form:

scheme://servername/.../basedir;*parameters*/subdir/.../file.extension.

32 The computer-readable medium of claim 7 wherein instruction (e) further includes the instruction of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

33 The computer-readable medium of claim 7 wherein instruction (e) further includes the instruction of: binding a combination of "basedir+path+sessionid" to an IP address of the client at first use of the URL ticket.

34 The computer-readable medium of claim 9 wherein instruction (g) further includes the instruction of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

35 The computer-readable medium of claim 1 further including the instruction of: ensuring that only the client that was issued the URL ticket can use the URL ticket by

(i) issuing a transfer ticket from the first server to the client when the first server needs to redirect the client to the second server,

(ii) recognizing by the second server the transfer ticket in a request from the client,

(iii) redirecting the client back to the second server with a URL ticket, and

(iv) verifying the ticket on the second server and returning the requested file.

36 The computer-readable medium of claim 1 further including the instruction of providing a content server as the first server and providing at least one replica server as the second server.

37 A URL ticket for redirecting a URL request for a file on a content server from a client to a replica server comprising:

a format in a form of

scheme://servername/.../basedir;*parameters*/subdir/.../file.extension.

where the "scheme" represents "http" or "https," and the "server name" represents a DNS name of the replica server, and wherein each parameter in the URL ticket includes a parameter name and a value:

name1=value1;name2=value2; ...

38 The URL ticket of claim 37 wherein the parameters include a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).